

**UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF MISSOURI**

JOHN AMBURGY, a Missouri resident,	)	
	)	
Plaintiff,	)	Civil Action No.:
	)	
v.	)	JURY TRIAL DEMANDED
	)	
EXPRESS SCRIPTS, INC., a Missouri	)	
Corporation, and DOES 1-9 inclusive,	)	
	)	
Defendants.	)	
	)	

**CLASS ACTION COMPLAINT**

Plaintiff John Amburgy ("Plaintiff"), on behalf of himself and all others similarly situated, hereby brings this class action suit against defendant Express Scripts, Inc. ("Defendants" or "Express Scripts") and DOES 1-9 inclusive (collectively, "Defendants"). Plaintiff makes the following allegations based upon personal knowledge, where applicable, and upon information and belief, and the investigation and research of Plaintiff's counsel:

**NATURE OF ACTION**

1. Plaintiff brings this class action suit on his own behalf, and on behalf of all entities and persons similarly situated, against Defendants, as a result of its failure to adequately safeguard its members' individually identifiable personal information (hereinafter "Confidential Information"). Such Confidential Information includes members' names, dates of birth, Social Security numbers and prescription information.
2. As a result of Defendants' failure to adequately protect and secure Plaintiff's and Class members' Confidential Information, unauthorized individuals gained access to Plaintiff's and Class members' Confidential Information (hereinafter the "Breach").

3. Defendants' failure to maintain reasonable and adequate security procedures to protect against the theft of Plaintiff's and other members of the Class members' Confidential Information has put them at an increased risk of becoming victims of identity theft crimes, fraud, abuse, and extortion. In addition, Plaintiff and the Class have spent (or will need to spend) considerable time and money to protect themselves as a result of Defendants' conduct.

4. Plaintiff and other members of the Class will suffer irreversible damage if their Confidential Information becomes public. As a proximate result of the Breach, millions of Express Scripts' members, including Plaintiff, have had their Confidential Information compromised, their privacy invaded, have been deprived of the exclusive use and control of their proprietary prescription information, have incurred costs of time and money to consistently monitor their credit card accounts, credit reports, prescription accounts, and other financial information in order to protect their Confidential Information, and have otherwise suffered economic damages.

#### **JURISDICTION & VENUE**

5. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one member of the class is a citizen of a different state than Defendants; there are more than 100 putative Class members nationwide; and the aggregate amount in controversy exceeds \$5,000,000. This Court has personal jurisdiction over the parties because Express Scripts has its principal place of business in this state, conducts substantial business in this state, has systematic and continuous contacts with this state, and has agents and representatives that can be found in this state. Plaintiff is also a resident of this state.

6. This Court has jurisdiction over the state common law claims pursuant to the doctrine of supplemental jurisdiction, as codified at 28 U.S.C. §1367(a).

7. Pursuant to 28 U.S.C. § 1391(a)(2), venue is proper in the Eastern District of Missouri because Express Scripts' headquarters are located in the Eastern District of Missouri.

### **PARTIES**

8. Plaintiff John Amburgy is a Missouri resident who is enrolled in the Line Construction Benefit Fund (hereinafter "Lineco"), a self-funded employee benefit plan. Plaintiff is a member of Express Scripts, because Express Scripts administers the prescription drug program for Lineco.

9. Express Scripts is a Delaware corporation with its corporate headquarters located at One Express Way, St. Louis, Missouri. Express Scripts provides a full range of pharmacy services, drug formulary management programs, and other clinical management programs for thousands of member groups, including managed care organizations, insurance carriers, third-party administrators, employers and union-sponsored benefit plans. Express Scripts is the third largest processor of pharmacy prescriptions, otherwise known as a pharmaceutical benefits management ("PBM") company.

10. Defendants DOES 1-9 are unidentified third party vendors that may collect and manage some of Express Scripts' member information. Plaintiff does not know the identities or locations of DOES 1-9 at this time. Plaintiff will amend his complaint when he learns the identities or locations of DOES 1-9.

### **FACTUAL BACKGROUND**

#### **Details of the Breach**

11. In early October 2008, Express Scripts received an "extortion letter," from an

unknown person or persons who had gained access to Express Scripts customers' Confidential Information. The extortionists demanded money from Express Scripts, in an amount which has not been disclosed to date, and threatened to publish the Confidential Information of millions of Express Scripts' members on the Internet if their demands were not satisfied. The extortion letter included the Confidential Information of approximately seventy-five Express Scripts members, including the members' names, dates of birth, Social Security numbers, and prescription information.

12. After refraining for nearly a month from notifying the public of the potential breach of their members Confidential Information, Express Scripts finally issued a statement on its website on November 6, 2008. The announcement about the above-mentioned extortion threat was vague, but noted that the company has refused to pay on any extortion demands and had contacted the FBI to investigate the case. *See Express Scripts Warns of Potential Large Data Breach Tied To Threat*, EXPRESS SCRIPTS SUPPORTS SITE, Nov. 6, 2008, <http://www.esisupports.com/esi-release110608/> (last visited Mar. 15, 2009).

13. Express Scripts released a second announcement on November 11, 2008, admitting that some of Express Scripts' members had directly received similar extortion letters, threatening to publish members' Confidential Information on the Internet if the extortionists' monetary demands were not satisfied. *See Express Scripts Reports New Threats Tied to Data Security Breach*, EXPRESS SCRIPTS SUPPORTS SITE, Nov. 11, 2008, <http://www.esisupports.com/esi-release111108/> (last visited Mar. 15, 2009). The number of Express Scripts members that have received these extortion letters has not been disclosed.

14. According to Steve Littlejohn, a spokesman for Express Scripts: "We know where the data came from by looking at it, but precisely how it was accessed is still part of

the investigation.” Brian Krebs, SECURITY FIX, Nov. 8, 2008, *Extortion Used in Prescription Data Breach; FBI Investigating Threat Against Express Scripts Customers*, <http://www.washingtonpost.com/wp-dyn/content/article/2008/11/07/AR2008110703434.html> (last visited Mar. 17, 2009).

15. Mr. Littlejohn also stated to the press that the company was not certain how much data had been stolen. See John Markoff, *F.B.I. Looks into a Threat to Reveal Patient Data*, NEW YORK TIMES, Nov. 6, 2008, [http://www.nytimes.com/2008/11/07/business/07data.html?\\_r=1&ref=business&oref=slogin](http://www.nytimes.com/2008/11/07/business/07data.html?_r=1&ref=business&oref=slogin) (last visited Mar. 17, 2009). He admitted that the company had not ruled out the possibility of an insider theft. See *id.* Mr. Littlejohn further stated that the company delayed publicizing the extortion letter to allow the investigation to take shape, but that it had now reached a stage where the company wanted to make it public. See Lewis Krauskopf, *Express Scripts reports extortion over data breach*, Reuters New York, Nov. 6, 2008, <http://www.reuters.com/article/ousiv/idUSTRE4A59FX20081106> (last visited Mar. 20, 2009).

16. Express Scripts’ “Frequently Asked Questions” page states, in response to the question: “How did it happen?”: “We believe we have identified where the data involved in this situation was stored in our systems and have instituted enhanced controls. We are continuing our investigation to identify those responsible for any unauthorized access.” Frequently Asked Questions, EXPRESS SCRIPTS SUPPORTS SITE, *available at* <http://www.esisupports.com/frequently-asked-questions/> (last visited Mar. 17, 2009).

17. Express Scripts knows where the stolen data was stored and, therefore, should be able to identify which members were affected by the Breach. However, nearly five months after receiving the extortion threat and many months after the occurrence of the data

security breach, Express Scripts has still not announced which and how many of its members have had their Confidential Information compromised as a result of the Breach. Other than to the 75 members whose names and Confidential Information were included in the extortion letter, Express Scripts has not, upon information and belief, provided individual notice of the Breach to the millions of people potentially affected by the Breach.

18. Express Scripts is in the best position to know who may have been affected by the Breach. As such, Express Scripts bears the duty of individually notifying its potentially affected members. Nonetheless, Express Scripts refuses to recognize any such duty

19. Due to the late notification by Express Scripts, and out of concern for its employees, the Fairfax County Public Schools system, an Express Scripts client, mailed a letter to its employees on November 7, 2008, alerting the health-plan participants of the Express Scripts Breach. The letter stated, "FCPS is deeply concerned about this kind of breach, which could adversely affect our employees. We expect and deserve the highest level of security when we entrust our vendors to handle our employees' personal information." *See* Blue Cross/Blue Shield Carefirst ESI Participant Message from Dr. Dale, FAIRFAX COUNTY PUBLIC SCHOOLS HUMAN RESOURCES, <http://www.fcps.edu/DHR/news/potentialbreachdrdaleletter.htm> (last visited Mar. 17, 2009).

20. Similarly, Northeast Utilities, the parent company of the Public Service of New Hampshire, and also a client of Express Scripts, sent a letter to its current and retired employees in November 2008 regarding the Breach. *See* Mark Hayward, *Security breach a prescription for fraud?* NEW HAMPSHIRE UNION LEADER, Dec. 3, 2008, <http://www.unionleader.com/article.aspx?headline=Security+breach+a+prescription+for+fraud%3F&articleId=e7e5420b-cbcf-45dc-8d26-064965e4c4ec> (last visited Mar. 17,

2009). One of Northeast Utilities' retired employees, John Linville, commented to the press on receipt of Northeast Utilities' letter that he was dismayed that although Express Scripts received the threat in early October, word was only getting out in late November/early December. *See id.*

21. Another Express Scripts client, the pension fund for retired nonunion employees of U.S. Steel, also alerted participants in November 2008 that their Confidential Information may be published on the Internet because of the theft of patient records from Express Scripts. *See* Torsten Ove, *U.S. Steel's pensioners warned about records theft*, PITTSBURGH POST-GAZETTE, Dec. 20, 2008, at A1 *available at* <http://www.post-gazette.com/pg/08355/936509-85.stm?cmpid=business.xml> (last visited Mar. 19, 2009). The spokeswoman for the U.S. Steel Carnegie Pension Fund stated that the fund was contacted by Express Scripts regarding the Breach and, shortly thereafter, U.S. Steel notified its participants of the potential danger from the Breach and referred all other questions to Express Scripts. *See id.* U.S. Steel stated in its letter that "we believe it is important for you to be aware of this situation so that you may be watchful for any fraudulent activity in your name." *Id.*

22. The Health Care Authority for Washington State Employees, who used Express Scripts as their pharmacy vendor between mid-2006 until 2007, also notified its participants of the Breach. *See* Brad Shannon, *Health care data may be breached Uniform Medical Plan vendor faced extortion threat*, OLYMPIAN, Dec. 9, 2008, *available at* <http://www.theolympian.com/southsound/story/692315.html> (last visited Mar. 19, 2009). The Spokesman for the Health Care Authority, Dave Wasser, stated that, "[n]one of those 75 are our people. But we don't have any way of knowing if our people could be in the (other)

data they claim to have.” *Id.*

23. The Uniform Medical Plan is the state-run health care option available to 170,000 state employees and dependents. *See id.* Unfortunately, Express Scripts did not provide details of the Breach or the stolen to Uniform Medical Plan: “We don’t know if it’s new data or old data or what kind of data these people took. It wouldn’t be credit card information. I suppose it could be Social Security numbers or something like that,” Wasser stated. *Id.* Wasser stated that it would be possible that some clients covered under the state-subsidized Basic Health Plan for the low-income working poor could be affected as well, and that the state of Washington is working with the Community Health Plan of Washington, which covers 60,000 Basic Health enrollees and also contracts with Express Scripts. *See id.*

24. Similarly, on November 21, 2008, the managing counsel of Toyota Motor Sales, U.S.A., Inc. mailed a letter to the New Hampshire Attorney General informing them of a data breach affecting approximately 23 New Hampshire residents. *See* Toyota Motor Sales, U.S.A., Inc. Notice to New Hampshire Attorney General’s Office, Consumer Protection Bureau, Nov. 21, 2008, *available at* <http://www.oag.state.md.us/idtheft/Breach%20Notices/ITU-161387.pdf> (last accessed Mar. 20, 2009). The letter stated that approximately one week after the November 6, 2008, announcement of the extortionists threat to Express Scripts, Toyota received a similar threat directly, apparently from the same extortionists, identifying 188 current and former Toyota associates’ names, Social Security numbers, and dates of birth held by Express Scripts. *Id.* Additionally, the extortionists suggested that they possessed similar information for “most” other current and former Toyota associates and their covered dependents. *Id.* Toyota stated that it sent an informal e-mail notice to affected employees on November 14, 2008, and that it would mail the formal notice

of security breach on November 20, 2008. The formal notice mailed to affected employees included, in bold-faced type:

**We believe that there is some risk, based on the threat contained in extortionists' letter, that you or your dependents' personal information could be misused. Therefore, we believe you should consider taking action to protect your identity even though, at this time, we have received no evidence that there has been any attempt to misuse your personal information or that of your covered dependents.**

*Id* (emphasis in original).

25. If Toyota received a letter from the extortionists identifying 188 current and former Toyota associates' names, Social Security numbers, and dates of birth as a result of the leak of this data by Express Scripts, then Express Scripts is, or should have been, aware that these participants were affected by the Breach and should have provided individual notice to these participants, or at least notice to Toyota that their employees' Confidential Information was compromised.

26. Companies like Toyota and their employee-participants are left in the dark regarding the impact of the Breach at Express Scripts. It is unclear how many more companies like Toyota have received direct extortion threats or how many participants have had their Confidential Information compromised.

27. In response to an article online about the Express Scripts Breach, a blog commenter, Roger Josek, stated:

Express Scripts has lost control of health- and credit-related data on millions of Americans, in what was almost certainly an inside job by one of their employees. Many levels of error and liability could exist on Express Scripts' part, from failing to take reasonable steps prevent unauthorized access to privacy data, to inadequate background checks of employment applicants. I went to the Express Scripts website and saw little to inspire confidence, were I one of the victims of the access

violation.

Roger Josek, November 7, 2008, Comment to Blog entry by Linda Tucci, *Express Scripts data breach includes demand for money, FBI brought in*, Nov. 7, 2008, <http://totalcio.blogs.techtarget.com/2008/11/07/express-scripts-data-breach-includes-demand-for-money-fbi-brought-in/> (last visited Mar. 19, 2009).

28. In response to the Express Scripts extortion announcement, other PBMs have assured its members that they have multiple data security measures in place to ward off similar attacks. See Neal Learner, *Express Scripts and Some of its Clients Face Extortion Attempts After Recent Data Breach*, AISHEALTH.COM, Dec. 3, 2008, available at <http://www.aishealth.com/Bnow/hbd120308.html> (last visited Mar. 19, 2009). For example, Medco Health Solutions, Inc. has institutionalized encryption technologies across the enterprise, and has conducted exhaustive reviews of all HIPAA-related data. See *id.* According to Medco Health Solutions, Inc. spokeswoman, Ann Smith's statement to the press: "all laptop and desktop computers and business-to-business information is encrypted, and the company has authentication and access control on its data, in addition to data security protocols that are proprietary ... 'We are obsessive and extreme on security with layers of backups.'" *Id.*

29. In response to the Express Scripts extortion announcement, CVS Caremark spokeswoman Christine K. Cramer stated to the press:

'CVS Caremark's security programs are robust and have many internal controls that are designed to prevent unauthorized access to confidential information' ... Key components of CVS Caremark's security program include the use of leading security technology, a comprehensive and consistently applied testing and validation program and strict protocols related to user access to confidential data.

*Id.* CVS Caremark Corporation, to its knowledge, has not received a letter similar to the one described by Express Scripts. *See id.*

30. Unlike its fellow industry members, Express Scripts has not announced what security programs, internal controls, and other data security measures it had or currently has in place to prevent unauthorized access to confidential information, nor why the extortionists were able to gain access to its members' Confidential Information.

31. The financial market has reacted to the egregious situation that Express Scripts members must face, as Express Scripts' share price fell approximately 6% on November 6, 2008.

32. Express Scripts' Chairman and Chief Executive Officer, George Paz, stated that despite the fact that Express Scripts "deploys a variety of security systems designed to protect their members' Confidential Information from unauthorized access ... as security experts know, no data system is completely invulnerable." Steve Ragan, *Express Scripts discloses extortion attempt and data breach*, THE TECH HERALD, Nov. 10, 2008, <http://www.thetechherald.com/article.php/200846/2422/Express-Script-discloses-extortion-attempt-and-data-breach> (last visited Mar. 19, 2009). Chairman Paz conceded that a breach of Express Scripts' data storage systems may be to blame for the theft of its members' Confidential Information. However, to date, the company has failed to formally announce the occurrence of a breach of its data systems or communicate to their members whether or not their Confidential Information was stolen. *See id.*

33. Harry Rhodes, a health information expert and director of practice leadership at the American Health Information Management Association, stated that "the [Express Scripts'] data breach behind the [extortion] threat doesn't represent the norm." Neal Learner,

*Express Scripts and Some of its Clients Face Extortion Attempts After Recent Data Breach*, AISHEALTH.COM, Dec. 3, 2008, available at <http://www.aishealth.com/Bnow/hbd120308.html> (last visited Mar. 19, 2009). Mr. Rhodes suggests that, following best practices, Express Scripts should publicize all of the measures it has taken to fix the problem. *See id.*

34. According to Mr. Rhodes, the public has a right to expect that their private health information will be protected. Now that Express Scripts has identified where the information came from in its database, Express Scripts stated that the company should be able to start zeroing in on the people that had access to that information: "They need to look at all of their employees, including their current employees." Mr. Rhodes further suggests: "The current best practice is [that] you do a background check on people who have access to this type of information, especially people who can download or move or copy large portions of information." *Id.*

35. Companies must perform risk assessments and continually monitor consumers' information and their employees. Mr. Rhodes added that:

Insiders post 80 percent of the risk, it makes sense to start security measures with employees. Companies should do background checks at hiring, throughout employment and when workers quit. Employers should ensure that no one has control of a process from beginning to end and should avoid falling into the trap of adding access authorization when someone is promoted without also deleting access the person no longer needs to do the job. Companies should monitor their systems for illicit activity and use electronic monitors that are always on guard, he said. It's also now common practice to minimize the use of Social Security numbers, by truncating them, avoiding their display or encrypting them.

*See id.*

36. Express Scripts was under a duty to implement and enforce security measures that would protect not only its members' identifying information, such as birth dates and

Social Security numbers, but also their confidential medical information:

Beyond the scale of the problem for Express Scripts — and the potential impact on the company is enormous — the issue extends well beyond the mounting concerns about identity theft, a phenomenon with which most people have become at least somewhat familiar. The greater problem is the unique nature of personal medical records, the importance of moving to computerization of such records to improve health safety and reduce costs and the irreversibility of the damage people can suffer if confidential medical information becomes public. The stakes are so high that a federal law establishes strict standards for maintaining the privacy of medical information and stiff fines for failing to do so. Medical records of all kinds — paper and, especially, electronic — must be protected with the most sophisticated kinds of security systems available, including backup protections and automatic alerts of security violations.

*See Not your Fathers' Data Breach, available at <http://1raindrop.typepad.com/>*

*1\_raindrop/2008/11/not-your-fathers-data-breach.html* (last visited Mar. 19, 2009).

37. According to Brian Krebs, a data security breach writer for the Washington Post, consumers have an expectation that the companies in which they entrust their personal information will protect and secure such sensitive information:

[T]he American people have the right to expect that their sensitive personal and medical information is zealously protected and kept secure — not only by Express Scripts but also by every person or company entrusted with it.... The Express Scripts breach raises many questions for all elements of the health industry: hospitals, clinics and doctors' practices, benefits management firms, insurance companies, pharmacies, employers and government agencies: Are they using the most advanced information security technology possible? Do they minimize the amount of data they collect and keep it only as long as necessary? Do they have strict protocols governing access to personal and medical data—and systems to enforce those protocols? If criminals were to hack into their systems, how would the companies know? How soon? And are the systems capable of instantly cutting off illegal access as soon as a breach is discovered?

*Id.*

38. Alan Paller, the director of research for the SANS Institute, a Bethesda,

Maryland based computer-security training group, has said that the health care industry is in many ways the perfect target for data breach extortionists. *See* Brian Krebs, *Extortionists Target Major Pharmacy Processor*, SECURITY FIX, Nov. 7, 2008, *available at* [http://voices.washingtonpost.com/securityfix/2008/11/extortionists\\_target\\_major\\_pha.html](http://voices.washingtonpost.com/securityfix/2008/11/extortionists_target_major_pha.html) (last visited Mar. 20, 2009). Mr. Paller stated that many companies, especially in the financial industry, have already paid extortionists to keep their customers' data from being released and that some companies have received more than one extortion threat a day. *Id.*

39. Information about how Express Scripts' data was compromised—and whether the theft could have been avoided—is in Express Scripts' exclusive knowledge and control and has not yet been disclosed to the public or its members. However, Express Scripts has stated, since announcing the extortion letter, that it is implementing stricter security controls over its systems. *See* Frequently Asked Questions, EXPRESS SCRIPTS SUPPORTS SITE, *available at* <http://www.esisupports.com/frequently-asked-questions/> (last visited Mar. 19, 2009) (“We [Express Scripts] believe we have identified where the data involved in this situation was stored in our systems and have instituted enhanced controls”).

40. Express Scripts' response to the extortion is insufficient. Express Scripts' informational website scantily describes the extortion situation, and gives little detail to its members as to whether their information was affected. Express Scripts has not acted in accordance with its obligations to protect its members' Confidential Information. Express Scripts should have: 1) prevented a breach of this magnitude from occurring in the first instance, 2) discovered the Breach prior to receiving the extortion threat, and 3) provided individual notice to its affected customers as soon as it discovered the Breach.

41. Express Scripts fails to identify when the unauthorized access occurred.

Although Express Scripts vaguely identifies that they received the extortion letter in “early” October, they do not reveal whether the access occurred immediately prior to that, or months, or even years earlier.

42. Express Scripts fails to identify why the company failed to detect the unauthorized access themselves, Express Scripts has also failed to identify how many members’ records were accessed. Neither has Express Scripts explained why the company stored members’ Social Security numbers and how many members had Social Security numbers stored on the accessed server.

43. Upon information and belief, the Confidential Information of at least one million of Express Scripts’ members was stolen from Express Scripts by unauthorized individuals. It is further believed that the unauthorized individuals sold Plaintiff’s Confidential Information, and/or will use the information to extort money from Plaintiff and other members of the Class.

#### **About Plaintiff**

44. Plaintiff is enrolled in Lineco, a multiemployer self-funded welfare benefit plan set up to provide medical, dental, vision, prescription and disability benefits, as well as life insurance, for outside members of the International Brotherhood of Electrical Workers. Self-funded plans are employee plans that pay claims using the plans’ money which is placed in a trust or similar account as assets of the employer.

45. Self-funded plans typically hire a third-party prescription benefits manager (“PBM”), such as Express Scripts, to administer the plan and to pay prescription drug claims for the employer, using the plan’s money.

46. When a covered participant in a self-funded plan fills a prescription at the

pharmacy, they present their prescription benefit and/or insurance card. The pharmacist submits the prescription drug claim online in real time to the PBM to be processed for eligibility, participant co-pay and pharmacy reimbursement. The PBM then bills the health care plan, which in turn remits to the PBM, which then in turn pays the dispensing pharmacy.

47. Lineco uses Express Scripts as its PBM.

**About Express Scripts**

48. Express Scripts derives its revenue primarily from the delivery of prescription drugs through its contracted network of retail pharmacies and mail pharmacy services. Express Scripts dispenses prescription drugs to members of the health plans that it serves primarily through its network of retail pharmacies.

49. More than 56,000 retail pharmacies, representing more than 99% of all United States retail pharmacies, participate in one or more of Express Scripts' networks. Express Scripts handles approximately 500 million drug prescriptions per year for approximately 50 million people and 1,600 American companies. Therefore, approximately one out of every six Americans has their prescriptions handled through Express Scripts. According to Express Scripts' website,<sup>1</sup> "[t]ens of millions of consumers count on Express Scripts to supply the information and treatment they need to maintain a healthy lifestyle."

50. Express Scripts' clients include a number of government agencies, including, the Office of the Director of National Intelligence (ODNI); Central Intelligence Agency (CIA); Defense Intelligence Agency (DIA); Department of Defense (DOD); Department of Energy, Office of Intelligence and Counterintelligence; Department of Homeland Security, Office of Intelligence and Analysis; Department of Treasury, Office of Intelligence and

---

<sup>1</sup> See <http://www.express-scripts.com/services/> (last visited Jan. 12, 2009).

Analysis; Drug Enforcement Administration, Intelligence Division; Federal Bureau of Investigation (FBI); National Geospatial Intelligence Agency (NGA); National Reconnaissance Office (NRO); Office of Naval Intelligence; State Department; U.S. Air Force, Office of Intelligence and Air Intelligence Agency; U.S. Army, Office of Intelligence and Security Command; U.S. Coast Guard, Office of Intelligence and Criminal Investigations; and the U.S. Marine Corps, Office of Intelligence and Marine Intelligence Activity.

51. This is not the first time that Express Scripts has been dishonest with its clients. For example, in 2004, Express Scripts was charged by the New York Attorney General with defrauding its consumers by asking doctors to switch their patients' drugs in order to gain bigger rebates from pharmaceutical companies, thereby enriching itself at the expense of its customers. *See* Melissa Davis, *Spitzer Takes Aim at Express Scripts*, THE STREET.COM, Aug. 4, 2004, [http://www.thestreet.com/\\_tscana/stocks/melissadavid/10176404.html](http://www.thestreet.com/_tscana/stocks/melissadavid/10176404.html) (last visited Mar. 19, 2009).

52. The New York AG case alleged that Express Scripts made misrepresentations during their 1999 contract talks regarding the amount of discounts Express Scripts could obtain for the state, which induced the Department of Civil Service into signing a contract. *See Attorney General Cuomo Secures \$27 Million Dollar Agreement to Crack Down on Pharmacy Benefit Managers Secretly Switching New Yorkers Prescription Drugs*, available at [http://www.oag.state.ny.us/media\\_center/2008/jul/july29a\\_08.html](http://www.oag.state.ny.us/media_center/2008/jul/july29a_08.html) (last visited Mar. 19, 2009). The lawsuit further alleged that Express Scripts inflated prices for generic drugs through various schemes and engaged in drug switching programs to get rebates from manufacturers. *See id.* Express Scripts also diverted manufacturer rebates to itself instead of

to the New York state employee's plan, which inflated the costs of prescription drugs in the plan. *See id.*

53. The investigation prompted lawsuits by 28 other states and the District of Columbia. Express Scripts eventually settled those cases for \$9.5 Million on May 27, 2008. *See* David P. Hamilton, *Express Scripts Fine Settles PBM Mess – For Now*, BNET, May 28, 2008, <http://industry.bnet.com/pharma/100080/express-scripts-fine-settles-pbm-mess-for-now/> (last visited Mar. 19, 2009).

54. The New York Attorney General's case, which also included the insurance company CIGNA, settled for \$27 million on July 29, 2008. *See Attorney General Cuomo Secures \$27 Million Dollar Agreement to Crack Down on Pharmacy Benefit Managers Secretly Switching New Yorkers Prescription Drugs*, available at [http://www.oag.state.ny.us/media\\_center/2008/jul/july29a\\_08.html](http://www.oag.state.ny.us/media_center/2008/jul/july29a_08.html) (last visited Mar. 19, 2009).

55. In 2005, Express Scripts was sued again for defrauding its clients when several self-insured ERISA plans brought a class action lawsuit against Express Scripts for breach of fiduciary duties. *See In re Express Scripts, Inc.*, 2008 WL 1766777, 3 (E.D.Mo. 2008). In providing PBM services, Express Scripts allegedly conducted itself in a manner contrary to its stated objective, *i.e.*, reducing costs, and instead engaged in a series of unlawful acts and/or omissions, which inflated the costs of pharmacy benefits, improperly steered plan participants toward certain drugs, and violated the participants' privacy, including:

(a) *Retaining Undisclosed Rebates from Manufacturers.* Express Scripts leveraged its buying power to negotiate favorable discounts, rebates, and other amounts from drug manufacturers; which undisclosed amounts were then retained.

*(b) Enriching Itself By Creating a Differential or “Spread” in Dispensing Fees and Discounts.* Retail pharmacy prices are based on the wholesale drug price and a dispensing fee charged by the pharmacy. Express Scripts negotiated discounted drug rates and dispensing fees, yet failed to pass or disclose all such amounts to Plaintiffs.

*(c) Enriching Itself through Favoring Specific Drugs and “Switching.”* Express Scripts retained undisclosed kickbacks from drug manufacturers in exchange for listing their drugs on formulary (the preferred medication list), or “switching” plan participants to certain drugs.

*(d) Enriching Itself through Circumventing “Best Pricing” Rules.* Express Scripts assisted manufacturers to distort and/or artificially inflate the average wholesale prices (“AWPs”) of their respective drugs.

*(e) Enriching Itself with Undisclosed Bulk Purchase Discounts on Mail Order Prescriptions.* Express Scripts received bulk purchase and/or prompt payment discounts from manufacturers, and failed to pass along (or disclose) such amounts to Plaintiffs.

*(f) Accounting Errors.* Express Scripts caused accounting errors by (i) paying claims outside eligibility; paying duplicate prescriptions; making erroneous dosing criteria; paying prescriptions outside refill parameters; making “dispense as written” errors; making prior-authorization errors; and making system-edit errors.

*See id.* (holding that the Plaintiffs adequately pled on these facts a claim for Breach of Fiduciary Duty under ERISA against the defendant, Express Scripts, and mandating the case to proceed to trial).

**Express Scripts’ Promises to Protect its Members’ Confidential Information in Compliance with HIPAA**

56. As a part of its general obligation as a business to protect its clients sensitive personal information, Express Scripts must also meet the requirements of Health Insurance Portability and Accountability Act (“HIPAA”). HIPAA sets strict guidelines to protect individually identifiable health information, and protect medical records of all kinds—paper and, especially, electronic—with the most sophisticated kinds of security systems available,

including backup protections and automatic alerts of security violations.

57. In marketing its services to members, Express Scripts has promised to maintain the privacy of members' Confidential Information pursuant to its obligations under federal law as enacted by the Health Insurance Portability and Availability Act ("HIPAA"). *See*, Express Scripts' Privacy Notice, *available at* <https://member.express-scripts.com/web/member/contact/privacy/noticePrivacyPractice.do> (last visited Mar. 19, 2009). Express Scripts promises to be compliant with all the applicable mandates of HIPAA, including but not limited to the following privacy specific provisions:

- a. Erection of physical and electronic barriers to safeguard individually identifiable health information;
- b. Receipt of authorizations from individuals as needed;
- c. Ability to make available to Health and Human Services internal books and records for purposes of determining member compliance with HIPAA Privacy requirements;
- d. Establishment of mechanisms to report to members any improper uses and disclosures of individually identifiable health information;
- e. Establishment of processes to provide individuals with access to their individually identifiable health information and the right to amend that information;

58. Due to the dangers of identity theft, federal and state legislatures have passed a number of laws in recent years to ensure that companies protect the security of sensitive Confidential Information in a company's files. Many of these laws include requirements for the handling of Confidential Information by health care providers, and also impose proactive obligations on companies to maintain reasonable security measures to protect an individual's Confidential Information.

59. Express Scripts has pledged its compliance with the federally mandated

standards in a Frequently Asked Questions pamphlet titled “General HIPAA Implementation FAQ”. *See* Express Scripts HIPAA Information, Frequently Asked Questions, *available at* <http://www.express-scripts.com/hipaa/faq/hipaaFAQ.pdf> (last visited Mar. 19, 2009).

60. HIPAA created national standards for transmitting electronic health care transactions, protecting patient privacy, and ensuring the security of individually identifiable health information. The Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”) establishes standards to protect individually identifiable health information, including restricting disclosures of protected health information to the minimum necessary for the intended purpose.

61. HIPAA also enacted security standards for protecting information, including: administrative safeguards to execute security measures to protect data and manage the conduct of personnel in relation to the protection of data; physical safeguards, including the protection of physical computer systems and the buildings holding such systems from inappropriate intrusion or removal; and technical safeguards to protect information, authenticate users, and control individual access to information.

62. With respect to compliance with the electronic security standards demanded under HIPAA, Express Scripts states that it is “dedicating significant resources to ensure that it complies with the newly finalized Security Standards and will take all appropriate steps to adequately ensure the confidentiality, integrity, and availability of all electronic protected health information it creates, receives, maintains, or transmits.” *See* Express Scripts HIPAA Information, Frequently Asked Questions, *available at* <http://www.express-scripts.com/hipaa/faq/hipaaFAQ.pdf> (last visited Dec. 5, 2008). Further, Express Scripts states that “technical administrative and physical safeguards are being reviewed and

implemented to assure that electronic member private health information transmitted to us is protected.” *Id.*

63. Express Scripts repeats that “encryption options are currently under analysis while network hardware configurations are being standardized to provide a secure environment. In addition, **network monitoring is being enhanced to detect potential security incidents.** ... Express Scripts has a contingency/disaster **plan to prevent unauthorized access to electronic protected health information ... and currently utilizes several levels of entity authentication and plans to enhance its entity authentication capabilities.**” (emphasis added). *Id.*

64. Upon information and belief, Express Scripts’ security systems did not meet the minimum level of protecting its members pursuant to HIPAA and its above-mentioned representations to protect its members’ Confidential Information, because it did not prevent against the Breach of millions of its members’ Confidential Information, let alone, according to its own announcement, learn that a breach of this nature and magnitude occurred until it received an extortion letter.

65. Upon information and belief, Express Scripts failed to use the most advanced information security technology available, did not minimize the amount of Confidential Information collected and stored on its members, did not have strict protocols to govern access to personal and medical data, failed to enforce those protocols, and failed to protect and screen against unauthorized access to those systems, as demonstrated by the unauthorized third parties’ ability to gain access to Express Scripts’ systems and their ability to view and download millions of members’ Confidential Information without any prohibition or detection.

**Express Scripts Directly Represents to its Members that it will Protect their Confidential Information**

66. In addition to promising to protect its members' Confidential Information in compliance with HIPAA, Express Scripts directly provides a notice of its privacy practices to its members.

67. When accessing their accounts online at <https://member.express-scripts.com/web/member/loginreg/loginStart.do>, in order to manage prescription benefits, obtain formulary information, or otherwise manage their account with Express Scripts, the member is provided with a direct link to Express Scripts' "Privacy Promise" page, which includes links to Express Scripts' Internet Privacy Promise and Express Scripts' Notice of Privacy Practices. *See* Privacy/Disclosure Statement, last revised May 29, 2001, *available at* <https://member.express-scripts.com/web/member/contact/privacy/internetPrivacyPromise.do> (last visited Mar. 20, 2009) [hereinafter "Privacy Promise"].

68. The Privacy Policy represents to members in pertinent part that Express Scripts is required by law to:

- maintain the privacy of your medical information
- provide you with notice of our legal duties and privacy practices with respect to your medical information
- abide by the terms of this Notice

69. The Privacy Promise represents to members in pertinent part that:

Express Scripts is firmly committed to protecting the confidentiality of your personal and medical information. When you enroll in an Express Scripts service, we ask for only the information required to meet your needs. Please understand that, when enrolling in a service, you are providing information on a voluntary basis. ... We have developed the following practices and policies to safeguard your information. ... When you register for an Express Scripts service or make service elections (such as choosing a prescription benefit package under your plan), you may voluntarily provide us with personal information, such as your name and e-mail address. When personal information is

combined with health or medical status information, we refer to it as “health-related personal information.” ... **Express Scripts will not sell or disclose your personal or health-related personal information** to other companies or organizations.

(emphasis added).

**Express Scripts Has a Duty to Protect its Members’ Confidential Information**

70. Express Scripts has a duty to protect its members’ Confidential Information.

71. Members’ Confidential Information includes names, dates of birth, Social Security numbers, and corresponding prescription information. Such information is a property interest owned by Express Scripts’ members and is not owned by Express Scripts.

72. Members trust Express Scripts to protect their Confidential Information for the limited purpose of providing prescription benefits. Members expect that their Confidential Information will not be disclosed except under limited and appropriate circumstances. Those circumstances are limited to processing health insurance and similar payment requirements, public health emergencies, and/or other narrow uses specified under HIPAA.

73. Express Scripts exercises discretionary authority and control over the administration and management of the plans, including how to secure its members’ Confidential Information and the limited circumstances under which disclosure of Confidential Information is permitted under HIPAA.

74. Express Scripts is obligated to discharge its duties for the exclusive purpose of providing benefits to participants and beneficiaries, and defraying reasonable expenses of administering the plans. Express Scripts is also obligated to act with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a

like character and with like aims.

75. Upon information and belief, Express Scripts failed to follow reasonable precautions to secure its members' Confidential Information, failed to provide timely notice, and failed protect its members from invasion of privacy, fraud, identity theft, abuse and extortion.

### **Consequences of the Breach**

76. As defined in the Fair and Accurate Credit Transactions Act of 2003, Pub.L. 108-159, Dec. 4, 2003 (FACTA), "identity theft" is a fraud that is committed or attempted when one person is using another person's identifying information without permission. Generally, identity theft occurs when a person's identifying information is used to commit fraud or other crimes. These crimes include credit card fraud, phone or utilities fraud, bank fraud, and government fraud. The FTC has stated that identity theft has been a serious problem in recent years, with approximately 9 million Americans falling victim to identity theft each year.

77. As the United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report"), more than 570 breaches involving theft of personal identifiers such as Social Security numbers were reported by the news media from January 2005 through January 2006. *See* <http://www.gao.gov/new.items/d07737.pdf> (last visited Mar. 20, 2009). These data breaches involve the "unauthorized or unintentional exposure, disclosure, or loss of sensitive Confidential Information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers."

78. Identity thieves use stolen Confidential Information such as Social Security

numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

79. In a pamphlet called "Identity Theft Repair Kit," the Office of the Attorney General of Colorado, John W. Suthers, outlines the immediate consequences of such a breach. An identity thief can then open a new credit card with the delinquent account reported on the victim's credit report. The imposter changes the mailing address on the victim's credit card account so that it will take some time before the victim realizes that there is a problem. The thief can establish phone or wireless service in the victim's name or open a bank account and use it to write bad checks. The thief can also file for bankruptcy to avoid paying debts or to avoid eviction. If arrested, the thief can give the police the victim's name, affecting their criminal record and subjecting the victim to arrest for not appearing in court. The thief can also make purchases related to illegal activities or take out an auto loan. *See* <http://www.ago.state.co.us/idtheft/idtrk.pdf> (last visited Mar. 20, 2009).

80. Identity theft crimes often include more than just crimes of financial loss. Identity thieves also commit various types of government fraud, such as: obtaining a driver's license or official identification card in the victim's name but with their picture; using the victim's name and Social Security number to obtain government benefits; or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or get medical services in the victim's name, and may even give the victim's Confidential Information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

81. Victims of identity theft often have a great deal of difficulty clearing their credit records, which can significantly impair their credit rating and ability to obtain loans.

While law enforcement, banks, credit bureaus, and collection agencies all have procedures to help identity theft victims, it can still take weeks, months, or years of effort and frustration to return to normal. A damaged credit history can also cause difficulty for the victim in obtaining a new job or renting an apartment, as employers and landlords often review credit records of new applicants. *Id.*

82. Identity theft victims spend numerous hours and money repairing damage to their good name and credit record. In addition, a person whose Confidential Information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office which conducted a comprehensive and extensive study of data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See <http://www.gao.gov/new.items/d07737.pdf> (last visited Mar. 20, 2009).

83. The American Civil Liberties Union, in response to the Express Scripts' Breach, reiterated its demand for the protection of individual privacy for all electronic medical records. Timothy Sparapani, the ACLU's Senior Legislative Counsel stated:

As we consider the switch from paper to electronic health records, this most recent investigation begs us to protect our medical privacy from a whole new level of identity theft. To extortionists, our personal health secrets are a commodity like any other. The federal government needs to ensure that we won't be left exposed and vulnerable if we go the Full Monty into the electronic world.

See ACLU Reacts to Extortion of Private Medical Records, Demands Protection and Urges Caution When Moving Into the Digital World, ACLU, Nov. 7, 2008, *available at* <http://www.aclu.org/privacy/medical/37726prs20081107.html> (last visited Mar. 20, 2009).

84. Thus, Plaintiff and other members of the Class now face years of constant surveillance, and monitoring to prevent further loss and damage.

#### **CLASS ACTION ALLEGATIONS**

85. Pursuant to Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure, Plaintiff bring this class action on behalf of himself and all other entities and persons similarly situated whose prescription benefit plan is administered by Express Scripts and whose Confidential Information was compromised as a result of the Breach (the "Class"). The Class does not include Express Scripts, its officers, directors, agents, or employees.

86. Upon information and belief, the Class is comprised of consumers, making the joinder of such cases impracticable. Disposition of the claims as a class action will provide substantial benefits to both the parties and the Court.

87. The rights of each member of the Class were violated in a similar fashion based upon Defendants' uniform wrongful conduct.

88. Defendants' conduct affected all Class members in the same manner. Defendants' failure to properly safeguard Class members' Confidential Information and failure to notify Class members of the Breach as soon as practical after the breach was discovered affected Plaintiff and the other members of the Class in a uniform manner.

89. Common questions of fact and law exist as to all members of the Class and predominate over any questions affecting solely individual Class members. Among the questions of fact and law that that predominate over individual issues are:

- a. Whether Defendants breached its duties to Plaintiff and other members of the Class by failing to secure the Confidential Information of its members;
- b. Whether Defendants breached its contract to protect its members' Confidential Information;
- c. Whether Defendants were negligent in collecting and storing Plaintiff's and other members of the Class' Confidential Information;
- d. Whether Defendants took reasonable steps and measures to safeguard Plaintiff's and other members of the Class' Confidential Information;
- e. Whether Defendants acted wrongfully by failing to properly safeguard its members' Confidential Information;
- f. Whether Defendants failed to notify Plaintiff and other members of the Class of the Breach as soon as practical after the Breach was discovered;
- g. Whether Defendants breached its duty to exercise reasonable care in storing Plaintiff's and other members of the Class' Confidential Information by improperly securing that information on its computer network.
- h. Whether Plaintiff and the other members of the Class are at an increased risk of identity theft, fraud, and extortion as a result of Defendants' failure to protect the Confidential Information of

Plaintiff and other members of the Class; and

- i. Whether Plaintiff and other members of the Class sustained damages, and if so, what is the proper measure of those damages.

90. Plaintiff's claims are typical of the claims of the other members of the Class they seek to represent, because Plaintiff's Confidential Information, like the Confidential Information of all members of the Class, was not adequately or reasonably secured by Express Scripts.

91. Plaintiff will fairly and adequately represent and protect the interests of the Class, in that he has no interest that is antagonistic to or that irreconcilably conflicts with those of other members of the Class.

92. Plaintiff has retained counsel competent and experienced in the prosecution of class action litigation.

93. This class action is fair and efficient and is the superior method of adjudicating the claims of Plaintiff and the Class for the following reasons:

- a. common questions of law and fact predominate over any questions affecting any individual Class member;
- b. the prosecution of separate actions by individual members of the Class would likely create a risk of inconsistent or varying adjudications with respect to individual members of the Class, thereby establishing incompatible standards of conduct for Defendants or would allow some Class members' claims to adversely affect other Class members' ability to protect their interests;
- c. Plaintiff is not aware of any other litigation of these issues ongoing in this

State or elsewhere brought by a nationwide class of members of Defendants;

- d. this forum is appropriate for litigation of this action because the cause of action arose in this District;
- e. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and
- f. the Class is readily definable, and prosecution as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

**COUNT I**  
**NEGLIGENCE**

94. Plaintiff incorporates by reference all the allegations set forth above as if fully set forth herein.

95. Express Scripts had a duty to use reasonable care to protect and secure Plaintiff's and Class members' Confidential Information within its possession or control.

96. Through their acts and omissions described herein, Defendants unlawfully breached their duty to use reasonable care to protect and secure Plaintiff's and Class members' Confidential Information within their possession or control.

97. Upon information and belief, the Confidential Information of Plaintiff and Class members was being improperly stored and inadequately safeguarded in violation of, *inter alia*, federal and industry rules and regulations at the time of the Breach.

98. Defendants had a duty to timely disclose the Breach and theft of the Confidential Information to Plaintiff and the Class so that they could take appropriate

measures to avoid unauthorized charges on their accounts, cancel or change account numbers, monitor their financial and health account information and credit reports for fraudulent charges, and take steps to prepare against any potential extortion attempts. Defendants breached this duty.

99. Defendants knew or should have known that their computer databases and network for storing Plaintiff's and Class members' Confidential Information and related information had security vulnerabilities. Defendants were negligent in continuing such data processing and storage in light of those vulnerabilities and the sensitivity of the data.

100. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class suffered damages including, but not limited to, monetary loss for fraudulent charges incurred on their accounts; fear and apprehension of fraud, abuse, extortion, loss of money, and identity theft; the burden and cost of monitoring their credit, bank and health insurance accounts and credit history; the burden and cost of closing compromised accounts and opening new accounts; the burden of closely scrutinizing credit card statements for past and future transactions; damage to their credit history; loss of privacy; fear of extortion and having their individually identifiable health information publicized, and other economic damages.

**COUNT II**  
**BREACH OF THIRD PARTY BENEFICIARY CONTRACT**

101. Plaintiff incorporates by reference all the allegations set forth above as if fully set forth herein.

102. Defendants contracted with members' employers to provide PBM services.

103. Express Scripts and the members' employers intended to benefit Plaintiff and Class members by providing prescription management services for their health insurance

programs and, as such, Plaintiff and other members of the Class are third-party beneficiaries of the contracts.

104. Upon information and belief, Plaintiff and Class members were the third party beneficiaries to contracts between members' employers and Plaintiff and Class members were damaged by the breach of those contracts ("PBM Contracts").

105. Upon information and belief, Defendants came into possession of Plaintiff's and Class members' Confidential Information for the sole purpose of obtaining prescription benefits and contracted to protect such information.

106. Upon information and belief, the PBM Contracts implied, in addition to the other requirements of the PBM Contracts, Defendants to not disclose Plaintiff's and Class members' Confidential Information to unauthorized third party entities, and to safeguard and protect the information from being compromised and/or stolen.

107. In marketing its services to members, Express Scripts promises to maintain the privacy of members' Confidential Information pursuant to its obligations under federal, law as enacted by the HIPAA, and promises to be compliant with all the applicable mandates of HIPAA.

108. Express Scripts promises that it complies with the electronic security standards demanded under HIPAA in providing its PBM services. Express Scripts states that it is "dedicating significant resources to ensure that it complies with the newly finalized Security Standards and will take all appropriate steps to adequately ensure the confidentiality, integrity, and availability of all electronic protected health information it creates, receives, maintains, or transmits." Further, Express Scripts states that "technical administrative and physical safeguards are being reviewed and implemented to assure that

electronic member private health information transmitted to us is protected.”

109. Express Scripts repeats that “encryption options are currently under analysis while network hardware configurations are being standardized to provide a secure environment. In addition, network monitoring is being enhanced to detect potential security incidents. ... Express Scripts has a contingency/disaster plan to prevent unauthorized access to electronic protected health information ... and currently utilizes several levels of entity authentication and plans to enhance its entity authentication capabilities.”

110. In addition to promising to protect its members’ Confidential Information in compliance with HIPAA, Express Scripts directly provides a notice of its privacy practices to Plaintiff and the members of the Class, when they login to their accounts online or otherwise access their accounts to manage their prescription benefits. The Privacy Notice represents to members that Express Scripts will “maintain the privacy of your medical information, provide you with notice of our legal duties and privacy practices with respect to your medical information, and abide by the terms of this Notice.” The Express Scripts Privacy Promise represents to members that, “Express Scripts is firmly committed to protecting the confidentiality of your personal and medical information. When you enroll in an Express Scripts service, we ask for only the information required to meet your needs. ... We have developed the following practices and policies to safeguard your information. ... When you register for an Express Scripts service or make service elections (such as choosing a prescription benefit package under your plan), you may voluntarily provide us with personal information, such as your name and e-mail address. When personal information is combined with health or medical status information, we refer to it as “health-related personal information.” ... **Express Scripts will not sell or disclose your personal or health-related**

**personal information** to other companies or organizations.”

111. Upon information and belief, Express Scripts’ security systems did not meet the minimum level of protecting its members pursuant to HIPAA, and its above-mentioned representations to protect its members’ Confidential Information, because it did not prevent against the Breach of millions of its members’ Confidential Information, let alone, according to its own announcement, learn that a breach of this nature and magnitude occurred until it received an extortion letter.

112. Defendants did not safeguard or protect Plaintiff’s and Class members’ Confidential Information from being compromised and/or stolen.

113. Because Defendants failed to safeguard and protect Plaintiff’s and Class members’ Confidential Information from being compromised and/or stolen, Defendants breached their contracts with members’ employers, for which Plaintiff and Class members were third party beneficiaries.

114. Plaintiff and Class members suffered and will continue to suffer actual damages, including but not limited to the cost and time spent on bank and credit monitoring, interest on unauthorized bank and credit charges, overdraft fees, identity theft, insurance fraud, anxiety, emotional distress, loss of privacy, and other economic and noneconomic harm. Plaintiffs and the Class members are entitled to damages as a result of Defendants’ breach of the PBM Contracts.

**COUNT III**  
**BREACH OF IMPLIED CONTRACT**

115. Plaintiff incorporates by reference all the allegations set forth above as if fully set forth herein.

116. Plaintiff and other members of the Class entered into implied contracts with

Defendants, such that Defendants agreed to properly safeguard their Confidential Information.

117. The implied contracts were based on, *inter alia*, Express Scripts' Privacy Policy and Privacy Notice, which stated that consumers' Confidential Information would be safeguarded from unauthorized individuals.

118. Without such implied contracts, Plaintiff and Class members would not have provided their Confidential Information to Express Scripts or managed their pharmaceutical benefits with Express Scripts.

119. Express Scripts breached its implied contracts by failing to maintain adequate data security.

120. Express Scripts and the members' employers intended to benefit Plaintiff and the other members of the Class by providing prescription management services for their health insurance programs and, as such, Plaintiff and other members of the Class are third-party beneficiaries of the Agreement.

121. Plaintiff and Class members suffered and will continue to suffer actual damages, including but not limited to the cost and time spent on bank and credit monitoring, identity theft, insurance fraud, anxiety, emotional distress, loss of privacy, and other economic and noneconomic harm.

**COUNT IV**  
**VIOLATION OF THE VARIOUS STATE DATA BREACH NOTIFICATION LAWS**

122. Plaintiff incorporates by reference all the allegations set forth above as if fully set forth herein.

123. Most states require organizations to promptly notify consumers whose

personal information has been exposed in a data breach. Eleven of those states allow affected consumers to recover for such a violation:

- California (Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82)
- Delaware (Del. Code tit. 6, § 12B-101 et seq.)
- District of Columbia (D.C. Code § 28-3851 et seq.)
- Hawaii (Haw. Rev. Stat. § 487N-2)
- Illinois (815 ILCS 530/1 et seq.)
- Louisiana (La. Rev. Stat. § 51:3071 et seq.)
- Maryland (Md. Code, Com. Law § 14-3501 et seq.)
- North Carolina (N.C. Gen. Stat § 75-65)
- Rhode Island (R.I. Gen. Laws § 11-49.2-1 et seq.)
- Tennessee (Tenn. Code § 47-18-2107)
- Washington (Wash. Rev. Code § 19.255.010)

124. Express Scripts came into possession of Plaintiff's and the other members of the Class' Confidential Information and had a duty to exercise reasonable care in safeguarding and protecting that information it did not own from being compromised and/or stolen.

125. Defendants had a duty to disclose the fact that Plaintiff's and the other members of the Class' Confidential Information within its possession had been, or was reasonably believed to have been, compromised in an appropriate amount of time given the situation at hand.

126. Defendants, through their actions and/or omissions, failed to promptly disclose the fact that Plaintiff's and the Class' Confidential Information within their possession had been, or was reasonably believed to have been, compromised.

127. Defendants' failure to promptly give notice of the breach of the security of its computerized data system violates the various statutes of the eleven (11) states as listed above.

128. Plaintiff and Class Members request that an injunction be issued to require Defendants to comply with the data breach notification statutes for each of the above-

referenced states and damages for each violation.

**COUNT V**  
**VIOLATION OF THE MISSOURI MERCHANDISING PRACTICES ACT**

129. Plaintiff incorporates by reference all the allegations set forth above as if fully set forth herein.

130. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the protection of the Plaintiff's and Class members' Confidential Information, Defendants violated the provisions of Section 407.020 of the Missouri Merchandising Practices Act.

131. Section 407.020 of the Missouri Merchandising Practices Act provides in pertinent part:

The act, use of employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce ... is declared to be an unlawful practice.

132. The term "merchandise" includes services, such as the PBM services provided by Defendant.

133. The acts and misconduct of Defendant Express Scripts alleged above violated the Missouri Merchandising Practices Act by, among other things, falsely promising to protect Plaintiff's and the Class members' Confidential Information in compliance with the above mentioned representations, failing to provide notice of the Breach to Plaintiff and the other members of the Class.

134. Plaintiff and the other members of the Class have lost property in the form of their Confidential Information. Missouri law recognizes various forms of intangible items,

including, upon information and belief, Social Security numbers and personally identifiable health information, such as names, dates of birth, and corresponding prescription information, which constitute property.

135. Because property is the exclusive right to use or possess a thing (or the exclusive ownership of that thing), property includes every intangible benefit and prerogative susceptible of possession or disposition. Confidential Information, particularly Social Security numbers, operates as a means of accessing financial accounts, and the means to access financial accounts is an intangible benefit susceptible of possession. Confidential Information thus constitutes property because it implies the right to use that Confidential Information, and it also implies the right to access funds in certain financial accounts. Confidential Information is thus a cognizable property interest.

136. Defendants' violation of the laws of this state and of common law by the practices complained of herein constitutes an unfair practice within the meaning of section 407.020 of the Missouri Merchandising Practices Act.

137. Defendants' requirement to transmit Social Security numbers over the Internet and attendant failure to encrypt or otherwise maintain reasonable security measures over such information it is not only unlawful but also constitutes an independent violation of the "unfair" prong of section 407.020 of the Missouri Merchandising Practices Act independent of the other causes of action asserted herein. Defendants' failure to adopt reasonable practices in protecting Confidential Information has resulted in Plaintiff and the Class spending time and money to protect against identity theft. Plaintiff and the Class are now at a higher risk of identity theft crimes. This harm sufficiently outweighs any of Express Scripts' justifications or motives for its practice of collecting and storing such information

without taking adequate and reasonable measures to protect such information.

138. As a result of Defendants' practices, Plaintiff and the Class have suffered a substantial injury-in-fact and have lost money or property. As a result of Defendants' failure to adopt, implement, and maintain reasonable security procedures, and through Defendants' unauthorized release of Confidential Information, Plaintiff and the other members of the Class have incurred costs and spent time associated with monitoring and repairing their credit. Further, Defendants' practices have increased Plaintiff and the other members of the Class risk of being victims of identity theft and other harm.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, individually and on behalf of all other entities and persons similarly situated, respectfully requests that the Court enter an Order:

- a. Certifying the proposed nationwide Class herein under Federal Rule of Civil Procedure 23(a) and (b)(3) and appointing Plaintiff as Class representative, and Plaintiff's counsel of record as Class counsel;
- b. Finding that Express Scripts breached its duty to safeguard and protect Plaintiff's and the other members of the Class Confidential Information stored on its computer network;
- c. Finding that Express Scripts' failure to promptly give notice of the breach of the security of its computerized data system violates the various data breach notification statutes of the eleven (11) above-referenced states and awarding damages for each violation;
- d. Declaring that Defendants' actions violated the Missouri

Merchandising Practices Act;

- e. Awarding all actual damages, statutory damages, penalties, and remedies available for the Defendants' violations of the Missouri Merchandising Practices Act;
- f. Awarding injunctive relief, including but not limited to: (i) the provision of credit monitoring and/or credit card monitoring services for the Plaintiff and other members of the Class; (ii) the provision of bank monitoring and/or bank monitoring services for the Plaintiff and the other members of the Class; (iii) the provision of identity theft insurance for the Plaintiff and the other members of the Class; (iv) the requirement that Defendants receive periodic compliance audits by a third party regarding the security of its computer systems used for processing and storing customer data is in compliance with federal and industry rules and regulations, including but not limited to the mandates under HIPAA; and (v) the requirement that Defendant notify all members affected by the Breach in compliance with the data breach notification statutes for each of the eleven (11) above-referenced states;
- g. Awarding the damages requested herein to Plaintiff and the Class;
- h. Awarding all costs, and expenses, including experts' fees, and attorneys' fees, and the costs of prosecuting this action;
- i. Awarding pre-judgment and post-judgment interest as prescribed

by law; and

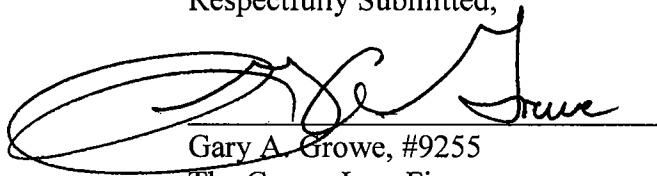
- j. Providing for other legal and/or equitable relief as is permitted at law and as justice requires.

**JURY TRIAL DEMANDED**

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: May <sup>8<sup>th</sup></sup> 2009

Respectfully Submitted,



Gary A. Growe, #9255  
The Growe Law Firm  
7733 Forsyth Blvd., Ste. 325  
St. Louis, MO 63105  
Telephone: (314) 725-1912  
Fax: (314) 261-7326

Of Counsel:

Mila Bartos  
Karen J. Marcus  
Shiva Sharifahmadian  
FINKELSTEIN THOMPSON LLP  
1050 30th Street, NW  
Washington, D.C. 20007  
Telephone: (202) 337-8000  
Fax: (202) 337-8090

Ben Barnow  
BARNOW AND ASSOCIATES, P.C.  
One North LaSalle Street, Suite 4600  
Chicago, IL 60602  
Telephone: (312) 621-2000  
Facsimile: (312) 641-5504